REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated August 2, 2005. Claims 28-31 are pending. Claims 1-16 are rejected. Claim 28 has been amended. Accordingly, claims 28-31 remain pending in the present application. A petition to extend the time to respond for one month from November 2, 2005 to December 2, 2005 is submitted herewith.

Claim 28 has been amended to recite that master secret key K and a secret key K_i are received "from a distribution center over a network after manufacture." Support for the amendment may be found throughout the specification, for example pages 1-3 and 6 -8. In particular, page 7, lines 3-5 describes the "...the key distribution center 24 distributes the cryptographic keys to the PGDs 14 and to the distribution centers 20 via a telecommunications network." Since FIG. 2 (and FIG.1 to which FIG. 2 is compared) show the PGDs 14 coupled between a distribution center and a distribution center, the distribution of the keys over the network clearly occurs after the PGDs have been manufactured. Accordingly, it is respectfully submitted that no new matter has been entered.

§103 Rejection

In the Office Action, the Examiner rejected claims 28-31 under 35 U.S.C. §103 (a) as being unpatentable over U.S. Patent Application No. 5,812,666 to Baker et al. in view of U.S. patent 6,058,193 to Cordery et al.

No Prima Facie Case Of Obviousness

To establish a prima facie case of obviousness, three basic criteria must be met: the prior art reference must teach or suggest all the claim limitations, there must be a reasonable expectation of success, and there must be some suggestion or motivation to modify the reference or to combine reference teachings. MPEP §2142. It is respectfully submitted that a combination of Baker and Cordery fail to teach or suggest the combination of elements recited in independent claim 28.

Baker provides a key management system that distributes cryptographic keys to digital meters for multiple domains, including vendor keys and postal keys for a plurality of countries. The key management system is configured to prevent translation of keys between domains, to provide assurance in a domain that the keys were generated in the domain, and that each key has been installed in only one meter by the system (col. 3, lines 23-31). The key management system includes separate logical security domains: one vendor domain and or one more postal domains. Each domain provides a full set of key generation, key distribution, key installation and token verification services (col. 5, lines 24-27). Vendor data keys are generated at a vendor data center (col. 5, lines 42-54), and postal keys are generated at a postal data center (col. 6, lines 5-14).

Both vendor and postal master keys are installed in the digital meters (col. 6, lines 43-47), and each digital meter receives the vendor master key and postal master key while physically located in the vendor manufacturing facility before distribution (col. 6, lines 52-56). To enforce a security requirement that a master key can only be attempted or installed in any digital meter once, each master key is identified by a domain master key identification number (col. 7, lines 18-58). Domain keys are used to

encrypt the domain master keys (vendor and postal) (col. 6, lines 61-63). The main keys are encrypted by domain Key set 103, which consist of a RSA key pair for confidentiality and an RSA key pair for authentication (col. 8, lines 4-15.)

In operation, each meter uses the domain master key to generate a temporal key, referred to as a token key for each domain, which is used to generate a token from mail piece data. Postal temporal keys distributed to postal verification sites are used for local verification of the indicia (col. 18, lines 23-34).

A. References Fail to Teach or Suggest All the Claim Limitations

It is respectfully submitted that the neither Baker or Cordery, singularly or in combination, teach or suggest the combination of elements recited in claim 28.

Referring to step (a), Baker fails to teach or suggest "receiving a master secret key K and a secret key K_i from a distribution center over a network after manufacture, and storing the master secret key K and the secret key K_i in the PGD," as recited in amended claim 28.

The Examiner cites column 6, lines 50-56 and column 9, lines 33-36 of Baker for disclosing the step. These passages, however, respectively state:

> A digital meter 36 receives the vendor master key and postal master key while physically located in the vendor manufacturing facility 14 **before distribution**, and
>
> The meter is securely configured so that **once keys are installed during manufacture**, they can never be removed or determined outside the manufacturing environment without leaving physical evidence of tampering.

Accordingly, Baker fails to teach or suggest PGDs "receiving a master secret key K and a secret key K_i ...over a network after manufacture," as recited in amended claim 28.

Referring to step (b) of claim 28, the Examiner cited column 16, line 60 through column 17, line 4; and column 17, lines 35-45 of Baker for disclosing "in response to receiving a request to generate an indicium for a mail piece destined for a particular postal destination *Dest*, generating the indicium."

However, column 16, line 60 through column 17, line 4 merely state:

> Referring now to FIG. 25, when a digital meter 36 is presented on the Manufacturing Line, the PSR computer 34 requests an install domain key record from the key distribution computer 30 at 330. At 330, Key Distribution Computer 30 sends an install domain key record to the PSR Computer in message MI4' which is further sent to Steel Box 32 at 334. Steel Box 32 queries the digital meter 36 for information, then at 336 sends the Domain Master Key in message MI5 to digital meter 36. The digital meter installs and checks the key and return status to Steel Box 32 which queries the digital meter for a set of Meter Test tokens. At 338, the Meter Test tokens are returned in message MI6 to...

And column 17, lines 35-45 merely state:

> Referring now to FIGS. 26 and 31, when the digital meter is prepared for a specific Security Domain, the Indicia Serial Number and/or Product Code Number is entered into the digital meter in message MR1. The PSR computer 34 requests registration tokens from digital meter 36 at 360. The digital meter generates two digital tokens and returns them the PSR computer at 362. The PSR computer combines the tokens with other meter information and forwards the resulting record to the Key Management Computer 24 through the Key Distribution Computer 30 at 364.

Both of these passages simply fail to describe indicium generation. Indeed, in the first passage the digital meter is still on the manufacturing line and cannot possibly be generating indicium for postage. Baker does discuss in column 18 using a domain Master Key to generate a temporal token key to generate a token (defined as a truncated result of encrypting indicia (col. 2, lines 6-7)) from mail piece data, but it is not believed that the token is signed as required in steps (c)-(f) of claim 28, discussed

below.

Referring to step (c) of claim 28, Baker fails to teach or suggest "computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination." The Examiner cites column 5, lines 38-42 and column 17, lines 28-44 of Baker for teaching this step. However, these passages respectively state:

> The digital meter calculates two proof of payment tokens, one using the vendor master key and the other using the postal master key. Failure in the verification of either digital token is sufficient proof of fraud. Referring now to FIG. 3, vendor data center 12 provides physical and information access control for Key Management System components.

> Key registration consists of associating the country of registration, and the indicia number with the product code number and the key. The key is then stored in the country sub-domain of the install domain using a secret key that is specific to the country sub-domain. The essential feature is that the brass process that is specific to that country sub-domain relies on the install domain to install keys securely and with integrity. Keys never transfer from one install domain to another.
>
> Referring now to FIGS. 26 and 31, when the digital meter is prepared for a specific Security Domain, the Indicia Serial Number and/or Product Code Number is entered into the digital meter in message MR1. The PSR computer 34 requests registration tokens from digital meter 36 at 360. The digital meter generates two digital tokens and returns them the PSR computer at 362. The PSR computer combines the tokens with other meter information and forwards the...

These passages cited by the Examiner have nothing at all to do with "computing a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination" and seem to be mistaken cites by the Examiner. Likewise, Baker also fails to teach or suggest the limitations of (d)-(f).

In the "Response to Arguments" section of the Office Action, the Examiner responded to Applicant's previous argument that Baker is not teach verification key's generate as a function of the secret key and postal destination and the verification keys are not used to create a digital signature, by citing the Background of Baker. The

Background of Baker teaches in general that in new digital meters, independent keys are used for generating digital tokens, and information about the meter and mail piece are combined and encrypted with vendor and postal master keys were keys derived therefrom (col. 2, lines 10-18). This discloses nothing more than what applicant disclosed in Applicant's Background of the invention, which states "when generating the IBI 22, the postage generating device 14 uses an internally generated private key and the public key to digitally sign the indicia, thereby creating a digital signature."

Applicant, however, is not attempting to claim the general notion of generating postage indicium with generated cryptographic keys. Instead, Claim 28 recites a specific implementation of computing keys to create a digital signature for indicia that is unobvious and has advantages over prior art approaches.

The present invention provides a method and system for dispensing and evidencing indicia by an indicia generating device in a system where a key distribution center divides the postage generating devices (PDGs) into n groups corresponding to different geographic designations (e.g., zip codes), and assigns a set of verification keys, V_i, to each PGD group, where each verification key in the set is encrypted as a function of one of the corresponding destination regions. The key distribution center also assigns a set of key ID's 23 to each PDG group, where each key ID in the set is associated with one of the assigned verification keys and is encrypted as a function of the same destination region used to encrypt the corresponding verification key. After assigning the verification keys 21 to the PGD groups 26, the KDC 24 distributes to each distribution center the sets of verification keys 21 and key ID's 23 that were encrypted as a function of the corresponding destination region.

The process begins when the PDG's receive a master secret key *K* and a secret

key K_i from the KDC. In response to receiving a request from a user to generate an indicium for a mail piece destined for a particular destination *Dest*, the indicium is generated, and the verification key V_i^{Dest} is computed as a function of the secret key K_i and the destination. The PGD also computes the encrypted key ID I_i^{Dest} as a function of the destination. The PGD evidences the indicia in step by creating a digital signature for the indicia using the verification key V_i^{Dest} and digitally signs the indicia by including the digital signature and the computed index I_i^{Dest} on the indicia. The mail piece bearing the postage indicia is now ready for mailing and subsequent verification. These are the steps recited in claim 28.

None of Baker's disclosed keys teach or suggest the keys and functionality of the keys described above and as recited in claim 28. For example, it is noted Baker discloses that a domain maser key is installed in each meter, and that each meter uses the domain master key to generate a temporal key, referred to as a token key, for each domain, which is used to generate a token from mail piece data. However, it is not believed either Baker's master key or the temporal key is analogous to the verification key.

Baker's master key is not analogous because it is installed during manufacturing, not received by the PGD "over a network after manufacturing." Because the domain master key is already present in the meter, it is also not computed as a function of "a secret key" and the postal destination, as required by step (c). The domain master key is also not used "to create a digital signature for the indicia", as recited in step (e). Instead, Baker's temporal key is used to generate the token from mail piece data. In addition, although Baker may teach that earth domain digital meters are assigned a country specific security domain and receive copies of earth domain

master keys that are encrypted with a country specific secret key, Baker fails to teach or suggest that meters in each group designation, "G_i, i = 1,...n", also receive "a secret K_i," corresponding to that Group designation, as required by step (a).

It is believed Baker's temporal key is not analogous to the claimed verification key because although the temporal key is computed from one key (the domain master key), it is not computed as a function of a second key, the "secret key", and the postal destination, as required by step (c).

Moreover, it is believed that Baker's country specific secret keys cannot be considered analogous to the recited secret K_i because Baker's country specific secret keys are not believed to be installed in the meters. In addition, Baker's country specific secret keys are not used by the meters to "comput[e] a verification key V_i^{Dest} as a function of the secret key K_i and the postal destination (*Dest*), as recited in step (c).

The Examiner relies on Cordery et al to cure the deficiencies of Baker. Cordery may teach the storing of a postal master key and a vendor master key in a meter and using the postal and vendor master keys to generate in the meter respective postal and vendor token keys that are then used to generate respective unique postal and vendor tokens that are date dependent. However, in Cordery there is no dividing the meters into groups. Therefore, there can be no distributing a master secret key K and a secret key K_i to the PGDs in the groups G_i, i = 1,...n, which in turn means there can be no "computing a verification key V_i^{Dest} as a function of the secret key K_i" and using the verification key to create a digital signature for the indicia.

B. Incorrect Motivation to Combine

In addition to the fact that a combination of Baker and Cordery fail to teach or

suggest all the limitations of claim 28, it is respectfully submitted that the Examiner also fails to state a prima facie case of obviousness because the motivation to combine the references stated by the Examiner is incorrect.

The Examiner stated "it would have been obvious to of ordinary skill in the art at the time the invention was made to modify the method of Baker et al. to use the generated verification key to create digital signature for the indicia, and digitally signing[sic] the indicia by including the digital signature and other generated token[sic] on the indicia because it would allow other party[sic] to determine whether both keys can be trusted that they actually originate from the meter." Office Action page 5.

The present invention, however, provides an improved method for evidencing and verifying postage indicia in which postage validation is performed at destination distribution centers, rather than at originating distribution centers, and the verification keys, which are encrypted as a function of the destination, are only distributed to the corresponding distribution centers. Thus, even if a destination center were broken into, the perpetrator would only be able to forge postal indicia for mail pieces destined for the particular destination. In addition, the key ID is also encrypted so that even if a perpetrator were to crack a verification key, the perpetrator would still have a problem identifying which verification key was obtained. In order to forge the indicia, the perpetrator must possess two keys, rather than one, a secret key that the PGD used to compute the key ID, and the verification key itself.

The Examiner's stated motivation to determine whether both keys can be trusted that they actually originate from the meter has nothing to do with increasing security of the evidencing and verifying postage indicia in the manner claimed.

Applicants' attorney believes this application in condition for allowance. Should

any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
Strategic Patent Group

December 2, 2005

/Stephen G. Sullivan/
Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 969-7474